## AMENDMENTS TO THE CLAIMS

This listing of claims will replace all prior versions of claims in the application:

1.-25. (Canceled)

26. (Currently Amended) An intrusion detection system, implemented using one or more computers, for detecting unauthorised use of a network, comprising:

a sniffer, implemented using the one or more computers, for capturing data being transmitted on said network; [[and]]

a pattern matching engine, implemented using the one or more computers for receiving data captured by said sniffer and comparing ~~said~~ the captured data with attack signatures for generating an event when a match between the captured data and at least one attack signature is found; and

a response analysis engine, implemented using the one or more computers and[[,]] triggered by said event, for comparing with response signatures [[the]] response data being transmitted on said network as a response to said data matched with said at least one attack signature and for correlating [[the]] results of said comparisons with attack and response signatures for generating an alarm.

27. (Currently Amended) The system of claim 26, wherein said response data ~~being transmitted on said network as a response to said data matched with said attack signature~~ is captured by said sniffer by performing an analysis of source IP address in data packets transmitted on said network.

28. (Currently Amended) The system of claim 26, wherein said response data ~~being transmitted on said network as a response to said data matched with said attack signature~~ is captured by said sniffer by performing an analysis of both source and destination IP addresses in data packets transmitted on said network.

29. (Currently Amended) The system of claim 26, wherein said response data ~~being transmitted on said network as a response to said data matched with said attack signature~~ is captured by said sniffer by analysing transport level information in data packets transmitted on said network.

30. (Currently Amended) The system of claim 26, wherein said response analysis engine generates [[an]] the alarm when said response data ~~being transmitted on said network as a response to said data matched with said attack signature~~ indicates that a new network connection has been established.

31. (Previously Presented) The system of claim 26, wherein said response signatures are arranged in two categories, response signatures identifying an illicit traffic, and response signatures identifying legitimate traffic.

32. (Currently Amended) The system of claim 31, wherein said response analysis engine generates [[an]] the alarm when a match between ~~captured~~ the response data and a response signature identifying illicit traffic is found.

33. (Currently Amended) The system of claim 31, wherein said response analysis engine comprises a counter which is incremented when a match between ~~captured~~ the response data and a response signature identifying legitimate traffic is found.

34. (Previously Presented) The system of claim 33, wherein, when said counter reaches a predetermined value, said response analysis engine terminates without generating any alarm.

35. (Previously Presented) The system of claim 26, wherein said response analysis engine comprises a time-out system triggered by said event for starting a probing task.

36. (Currently Amended) The system of claim 35, wherein said probing task verifies if any data has been detected on said network as [[a]] the response to said data matched with said at least one attack signature and, if such condition is verified:

generates [[an]] the alarm in case only response signatures indicating legitimate traffic have been used by said response analysis engine; or

ends the probing task in case only response signatures indicating illicit traffic or both response signatures indicating legitimate traffic and illicit traffic have been used by said response analysis engine.

37. (Currently Amended) The system of claim 36, wherein, if such condition is not verified, said probing task attempts to perform a connection to a suspected attacked computer, for generating [[an]] the alarm if such attempt is successful, or for ending the probing task if such attempt is unsuccessful.

38. (Currently Amended) A method performed using one or more computers for detecting unauthorised use of a network, comprising ~~the steps~~:

capturing data, using the one or more computers, being transmitted on said network;

comparing ~~said~~ the captured data with attack signatures for generating an event, using the one or more computers, when a match between the captured data and at least one attack signature is found; and

when triggered by said event[[;]]:

comparing with response signatures [[the]], using the one or more computers, response data being transmitted on said network as a response to said data matched with said at least one attack signature; and

correlating [[the]] results of said comparisons, using the one or more computers, with attack and response signatures for generating an alarm.

39. (Currently Amended) The method of claim 38, wherein said response data ~~being transmitted on said network as a response to said data matched with said attack signature~~ is captured by performing an analysis of source IP address in data packets transmitted on said network.

40. (Currently Amended) The method of claim 38, wherein said response data ~~being transmitted on said network as a response to said data matched with said attack signature~~ is captured by performing an analysis of both source and destination IP addresses in data packets transmitted on said network.

41. (Currently Amended) The method of claim 38, wherein said response data ~~being transmitted on said network as a response to said data matched with said attack signature~~ is captured by analysing transport level information in data packets transmitted on said network.

42. (Currently Amended) The method of claim 38, comprising the step of generating [[an]] the alarm when said response data ~~being transmitted on said network as a response to said data matched with said attack signature~~ indicates that a new network connection has been established.

43. (Currently Amended) The method of claim 38, wherein said response signatures are arranged in two categories, response signatures identifying illicit traffic, and response signatures identifying legitimate traffic.

44. (Currently Amended) The method of claim 43, comprising the step of generating [[an]] the alarm when a match between ~~captured~~ the response data and a response signature identifying illicit traffic is found.

45. (Currently Amended) The method of claim 43, comprising the step of incrementing a counter when a match between ~~captured~~ the response data and a response signature identifying legitimate traffic is found.

46. (Previously Presented) The method of claim 45, wherein said step of comparing data with response signatures is terminated when said counter reaches a predetermined value.

47. (Previously Presented) The method of claim 38, comprising the step of providing a time-out system, triggered by said event, for starting a probing task.

48. (Currently Amended) The method of claim 47, comprising the step of verifying if any data has been detected on said network as a response to said data matched with said at least one attack signature, and, if such condition is verified:

generating [[an]] the alarm in case only response signatures indicating legitimate traffic have been used; or ending said probing task in case only response signatures indicating illicit traffic or both response signatures indicating legitimate traffic and illicit traffic have been used.

49. (Currently Amended) The method of claim 48, wherein, if such condition is not verified, said probing task attempts to perform a connection to a suspected attacked computer, for generating [[an]] the alarm if such attempt is successful, or for ending the probing task if such attempt is unsuccessful.

50. (Currently Amended) A computer readable medium encoded with a computer program product ~~capable of being loaded~~ loadable into a ~~in the~~ memory of at least one computer, the computer program product ~~and~~ including software code portions for performing the method of any one of claims 38 to 49 ~~when the product is capable of being run on a computer~~.